QUALITY-OF-PROTECTION-DRIVEN DATA FORWARDING FOR INTERMITTENTLY CONNECTED WIRELESS NETWORKS

DAPENG WU, HONGPEI ZHANG, HONGGANG WANG, CHONGGANG WANG, RUYAN WANG, AND YI XIE

idea性质的陈述

几篇参考文献 可能很好

ABSTRACT

The data delivery in ICWN is accomplished in a collaborative manner, and non-cooperative behavior will gravely impair network QoP and user QoE. To select reliable relay nodes for data transmission, a trust-status-aware data forwarding strategy is proposed in this article. By exploiting locally recorded forwarding behavior information, process-based and relationship-based credibility can be precisely evaluated in a distributed manner. Additionally, with the assistance of an effective intrusion detection mechanism, reasonable relay selection can be perfected. Numerical results show that the proposed mechanism can provide reliable data transmission with high QoP and improved user QoE, which dramatically reduces the network load and enhances the resource utilization.

INTRODUCTION

Different from mobile ad hoc networks (MANETs), an intermittently connected wireless network (ICWN) avoids establishing a complete end-to-end path beforehand, and instead employs the store-carry-forward method to forward data hop by hop, which assists communications in highly dynamic and intermittently connected networks. As an emerging mobile network, the ICWN, proposed by the Internet Research Task Force (IRTF), is an improved version of a delay tolerant network (DTN) and inherits its general features [1]. Compared to a DTN, an ICWN emphasizes the intermittent connection characteristic caused by frequent node movements. To guarantee a favorable quality of experience (QoE) for users, data delivery in an ICWN is even more challenging [2].

Compared to quality of service (QoS), QoE focuses on the subjective experience of users during the service process: the comfort level or accessibility [3]. However, in an ICWN with highly dynamic topology, data delivery is assisted by multiple relay nodes cooperatively. Due to frequently disrupted link connections, nodes store and carry received data while moving, and wait for a proper forwarding opportunity. Thus, a reasonable design of the data forwarding mechanism is crucial to optimization of the user QoE and network performance [4]. A general data forwarding process in ICWN is shown in Fig. 1.

However, nodes are occasionally unwilling to help forward the received data and even negatively drop them because of their social relationships, limited resources, and privacy protection. These non-cooperative types of behavior can severely affect the network performance, and research shows that the proportion of non-cooperative nodes is determinant [5]. Obviously, the existence of non-cooperative nodes will affect the user QoE. As network security is drawing more and more attention from users, non-cooperative behaviors will undermine the network availability and scalability. Therefore, an effective trust mechanism is demanded to improve the network reliability, security, privacy, and QoE. To evaluate the efficacy and reliability of the security mechanism, researchers have proposed the concept of quality of protection (QoP) [3], which has not been clearly defined. Reference [6] proposed a security evaluation method based on node behaviors and reliable evidence gathering, and defined the reliability of the data transmission as QoP, that is, the network availability and reliability under attack. Therefore, improving the network QoP can benefit the user comfort level with the network service (i.e., QoE). Nevertheless, in a resource-limited ICWN, the challenge of guaranteeing QoP is that the trust status cannot be accurately evaluated according to node behavior. Besides, the additional communication overhead brought by the trust evaluation process inevitably affects the

Dapeng Wu, Hongpei Zhang, and Ruyan Wang are with Chongqing University of Posts and Telecommunications.

Honggang Wang, who is the corresponding author for this article, is with the University of Massachusetts Dartmouth.

Chonggang Wang is with InterDigital Communications.

Yi Xie is with the China Academy of Telecommunication Research of MIIT.

1536-1284/15/$25.00 © 2015 IEEE

user QoE. Ultimately, ensuring QoE and QoP of data forwarding is crucial to network performance improvements [7].

Due to the limited node capability, sparse node distribution, and dynamic network topology, the trust status cannot be evaluated accurately based solely on the direct interaction between nodes. Therefore, indirect trust information obtained in the moving process should be considered to more objectively, rapidly, and accurately estimate the node credibility, and to consequently enhance the network QoP [8].

Aiming to eliminate the negative impacts of non-cooperative behaviors on data forwarding strategies and enhance the network QoP, researchers have proposed various solutions. In [9], encounter tags with time stamps and private key signatures are utilized by nodes to verify the encounter history information, so service ability and credibility can be estimated, and data forwarding can be accordingly accomplished. However, the trust status cannot be accurately reflected only based on the encounter information, and the positive collaboration model assumption lacks reasonability. Reference [10] utilizes a positive forwarding message (PFM) to verify the forwarding behavior. Through the hop-by-hop feedback of the PFM and with the assistance of node signatures, malicious forging and changing of a PFM are prohibited. However, the control overhead is too heavy for its realization. To mitigate the impact of malicious feedback behavior, [11] estimates and aggregates the feedback through the hidden Markov model and Coleman fusion method. By simultaneously auto-calibrating the dynamic model parameters using the expectation maximization algorithm, the impacts of malicious feedbacks can be alleviated, which also induces high computational complexity and has restricted scalability. Reference [12] proposed fuzzy quantification on node credibility to detect malicious nodes, evaluate the trust status, and select the best relay through a predefined threshold and an iteration algorithm. But the fixed threshold fails to suit the dynamic topology, and the fuzzy quantification lacks accuracy. Reference [13] defines and detects malicious recommendation messages according to a predefined threshold. Through iteration, malicious recommendation messages can be filtered and discarded. Its effectiveness depends on the threshold setting and is also unsuitable for the highly dynamic ICWN.

Besides, actual measurements show that ICWN has the distinct feature of "big world, small world," and nodes are socially related [14]. According to the relationship strengths between nodes, a network can be logically divided into communities, where nodes of the same community have tight relationships and meet frequently. Obviously, factors such as the topology structure, buffer size, energy resource, social attribute, and non-cooperative behavior are considered to devise the data forwarding mechanism for a reasonable relay selection and better network QoP and QoE. Therefore, the design of an effective forwarding mechanism is a major research challenge for ICWN.

Additionally, the trust relationship between nodes is not only related to the interaction history, node behaviors, and evidence information, but is also affected by their social attributes. The node credibility can be evaluated according to the historical node behaviors, and nodes in an ICWN always help forward data for socially close nodes. Thus, both process-based and relationship-based credibility should be taken into account, where process-based credibility measures negative forwarding and malicious discarding of data, and relationship-based credibility is related to social attributes. Besides, due to the limited node interaction opportunities, the recommendation information from neighbor nodes is also utilized to assess the credibility. Finally, an effective intrusion detection mechanism is designed to filter the malicious recommendation messages and eliminate the influence of malicious nodes.

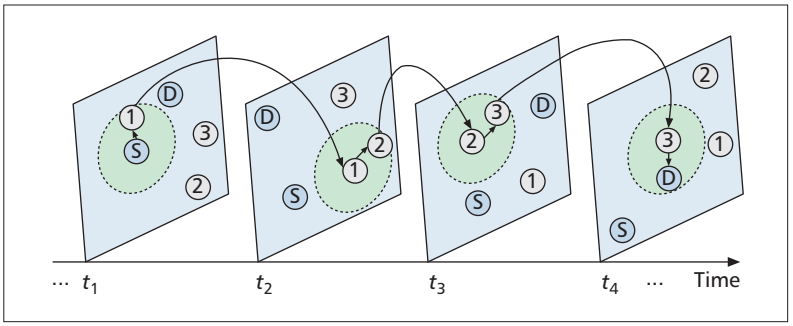

Figure 1. General data forwarding process in an ICWN.

A QoP-driven data forwarding (QoP-DF) strategy is proposed to enhance the QoP for an ICWN in this article. According to the encounter history, the encounter frequency between nodes can be calculated. Moreover, the relationship strengths between neighbors can be estimated according to the encounter frequency. Thus, the relationship-based and process-based credibility can be evaluated. With the assistance of an intrusion detection mechanism, malicious nodes can be distinguished to further mitigate the influence of non-cooperative behavior. Combining recommendation messages from neighbors, data can be reasonably forwarded in a distributed manner.

The main contributions of this article are presented below.

First, an effective security scheme is introduced to enhance network QoP, and a holistic approach to security evaluation based on the system reliability and service overhead is proposed.

Second, a node credibility evaluation mechanism for ICWNs is introduced to determine the different node status. By exploiting the locally recorded forwarding behavior information, process-based credibility can be precisely evaluated in a distributed manner. In addition, by analyzing the node movement law and service similarity, relationship-based credibility can be evaluated precisely. Due to various node encounter strengths, an adaptive weight factor is designed. In addition, by considering the node credibility, a hybrid and dynamic trust evaluation mechanism is designed.

Last, a node social relationship strength evaluation method is designed according to the his-

Similar to the trust between people in real life, node credibility can be classified into process-based and relationship-based credibility, where process-based credibility reflects cooperative behavior, and relationship-based credibility measures trust built on social topology.

torical movement information. By comparing the connection duration and connection times, the neighbors of a given node can be determined. Consequently, the social relationship strength between nodes can be determined according to the number of common neighbors.

The remainder of this article is organized as follows. In the next section, the relationship strengths between nodes is introduced. In the third section, based on the social relationships between nodes and forwarding behavior, the node credibility evaluation mechanism is designed thoughtfully. Following that, the trust status aware data forwarding mechanism is proposed. Then we evaluate the performance of the proposed data forwarding mechanism, and compare it with previous works. Finally, the conclusion and acknowledgment are given, respectively.

Relationship Strengths between Neighbors

Nodes are socially interrelated in an ICWN. Due to their stable relationships, communities are logically formed by closely related nodes in a self-organized manner [15]. Apparently, obtaining the network topology structure is prerequisite to designing an effective data forwarding strategy and improving user QoE.

Through the assistance of neighbor nodes, data can be rapidly forwarded, which implies that the topology structure detection helps improve the network service quality. Obviously, neighbors encounter each other frequently, and both the encounter times and connection durations should be considered to evaluate the encounter strength. The encounter strength between node i and $jQ(i, j)$ denotes the product of the average connection duration

$$dur_i^j(t)/t$$

and the encounter times $n_i^j(t)$, where $dur_i^j(t)$ is the total connection duration.

As mentioned above, the high encounter frequency and long connection duration lead to high encounter strength. Thus, the encounter strength can be utilized to define neighbor nodes, and the neighbors of node i are defined as the nodes that have encounter strength with node i not less than Q_{ave}, where Q_{ave} is the average encounter strength of node i. Finally, the neighbor set of node $i\Gamma(i)$ can be constructed.

According to the "weak ties" theory in social networks, the relationship strength between two remote nodes can be enhanced through their mutual neighbors. To achieve the data exchange for two remote nodes under the circumstance in which they share no mutual neighbors, the node relationship strength $b_{i,j}(t)$ is defined as $e^{\alpha-1}$, where

$$\alpha = \left[dur_i^j(t) \Big/ \sum_{k=1}^{n_i^N(t)} dur_i^k(t) \right] \cdot \frac{|\Gamma(i) \cap \Gamma(j)|}{|\Gamma(i)|}$$

and $n_i^N(t)$ is the number of encountered nodes. When two nodes never meet and have no mutual neighbors, their relationship strength is set to 0.

Node Credibility Evaluation

To improve the network QoP, the accurate estimation of node credibility is indispensable to handle non-cooperative behaviors. Similar to the trust between people in real life, node credibility can be classified into process-based and relationship-based credibility, where process-based credibility reflects the cooperative behavior, and relationship-based credibility measures trust built on social topology. Therefore, by analyzing the above two credibility types, the node trust status can be accurately evaluated, and relay nodes can be reasonably selected to further enhance the reliability of data forwarding.

For effective evaluation node credibility, its value is defined as the variable between [0,1], where 0 indicates complete distrust, 0.5 for unknown trust status, and 1 denotes full trust. The credibility evaluation value of node j at time t is denoted by $T_{i,j}(t)$, and it is under the combined effect of node behaviors and social attributes, that is, $T_{i,j} = \beta \cdot T_{i,j}^{beh}(t) + (1 - \beta) \cdot T_{i,j}^{s}(t)$, where $T_{i,j}^{beh}(t)$ and $T_{i,j}^{s}(t)$ denote process-based and relationship-based credibility, respectively, and β is the weight factor.

Process-Based Credibility Evaluation

Malicious nodes in an ICWN constantly tail other nodes to promote their activity degrees, and to further intercept transmitting data and discard them viciously. Meanwhile, malicious nodes spread forged trust recommendation messages to aggravate network performance. Therefore, the successful forwarding times and number of forged recommendation messages are considered to calculate $T_{i,j}^{beh}(t)$.

To precisely verify successful data forwarding, a hop-by-hop feedback mechanism is adopted to verify successful packet forwarding [10]. Also, the downstream active feedback is employed to avoid feedback data loss, that is, when data from upstream nodes are successfully received, downstream nodes will immediately send back the corresponding acknowledge message. If timeout occurs, the discarding times $f_{i,j}$ increase by 1; otherwise, the forwarding times $r_{i,j}$ increase by 1. For a resource-limited and highly dynamic ICWN, maliciously discarding data and intentionally spreading forged recommendation messages will severely waste the network resources and encounter opportunities. Thus, once discarding is detected, $T_{i,j}^{beh}(t)$ will be deducted according to the attack times. To accurately depict the trend of process-based credibility, the exponential function and arc tangent function are adopted: $1/\pi \arctan r_{k,m}$ and $(1/2)e^{-f_{k,m}}$. For extremely malicious nodes and cooperative nodes, their process-based credibility tends to be 0 and 1 correspondingly.

Furthermore, to detect forged recommendation messages, nodes request the estimated process-based credibility of the encountered node from neighbors. Upon receiving the recommendation messages, the process-based credibility $T_m^{beh}(t)$ of node m can be calculated by the weighted average method, the ratio of

$$\sum_{j \in C_i} \left\{ T_{i,j}(t) \times T_{j,m}^{beh}(t) \right\} \text{ to } \sum_{j \in C_i} T_{i,j}(t).$$

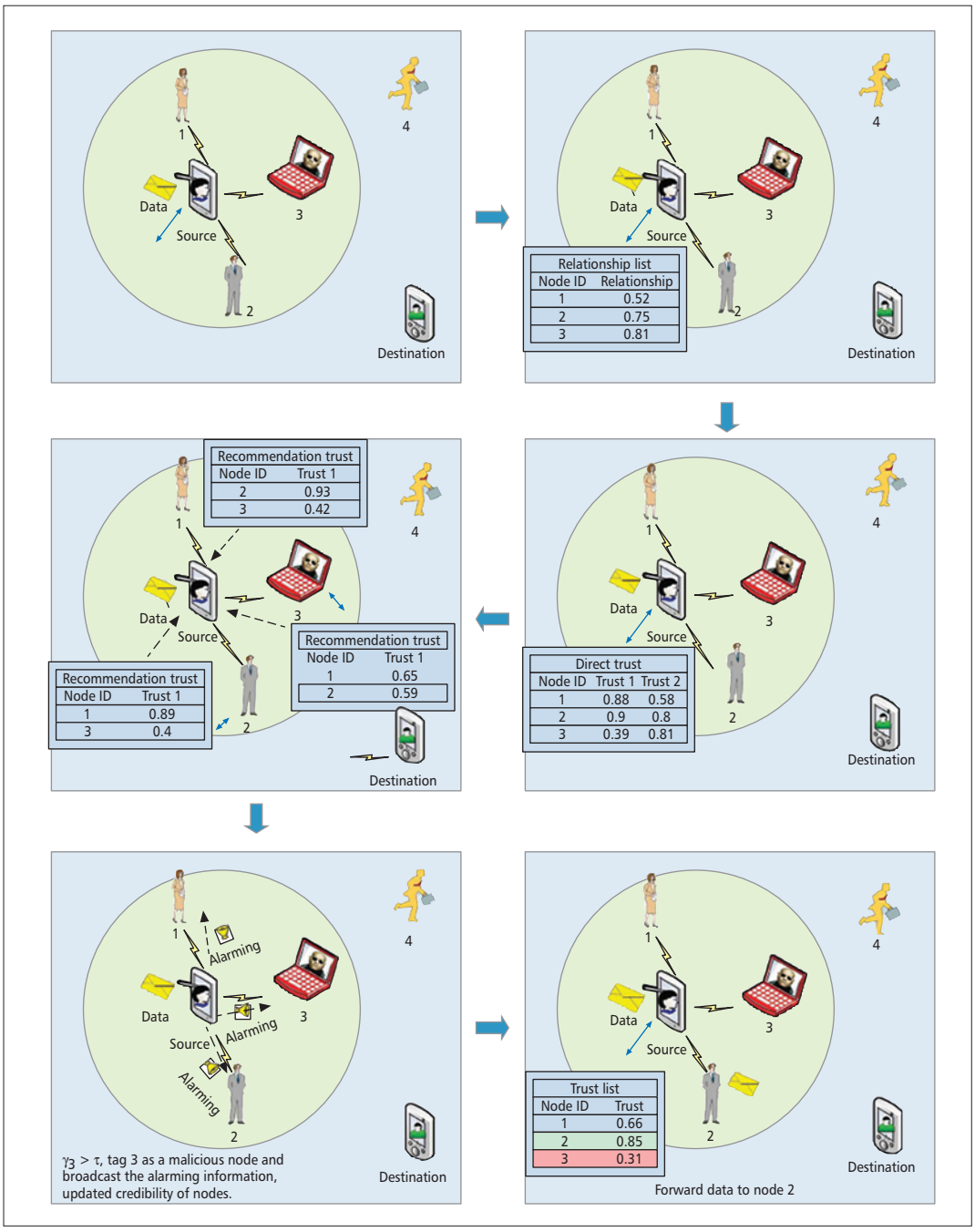

Figure 2. Illustration of QoP-driven data forwarding.

The standard deviation is the metric for statistical distributions and can approximately reflect the average deviation degree of the statistics. Therefore, the standard deviation of all recommendation messages serves as the threshold to detect the malicious behaviors.

不一致性超过阈值// 可能是blackend

C_i is the neighbor set of node i, and node i calculates the inconsistency γ_k between credibility values according to the product of the recommendation difference and the time factor $\hat{\lambda}^{t-t_{k,m}}$, where $\hat{\lambda}$ is the time attenuation factor, t denotes the current time, and $t_{k,m}$ is the credibility update time from node k to m. If the inconsistency γ_k exceeds the given threshold, which implies that node k has maliciously blackened the credibility of node m to waste the network resources, the credibility of node k is updated by node i to tag it as a malicious node, and the updated credibility of node k is broadcast to the neighbors of node i. Otherwise, the aggregated credibility $T_m^{beh}(t)$ is regarded as the process-based credibility of node m.

Obviously, a reasonable selection of the threshold τ is crucial to malicious behavior detection. Thus, a dynamic threshold is necessary for an ICWN due to the rapidly changing topology. The standard deviation is the metric for statistical distributions and can approximately reflect the average deviation degree of the statistics. Therefore, the standard deviation of all recommendation messages serves as the threshold to detect malicious behavior.

动态阈值

用标准差 作为 阈值

Relationship-Based Credibility Evaluation

Apparently, relationship-based credibility is calculated according to the node trajectory and network topology, which measures the trust relationship based on node similarity. Nodes

```
while node encounter do
  Public void SocialRelations() {
  Calculate EncounterDegree;
  Update NeighbourList;
  Update SocialRelations;
  }
  Public void Credibility() {
  Calculate credibility of node;
  ReqforRec(); // request recommendation message from neighbor;
  Detect malicious node;
  Update credibility of node;
  }
  Public void Forwarding(){
  if (Credibility of node j) < 0.5} then
     Wait for suitable Node;
  else if (Credibility of node j ) > (Credibility of node i) then
     Forwarding data to node j;
  else if SocialRelations(j, d)  > SocialRelations(i, d) then
     Forwarding data to node j;
  else
     Wait for suitable node;
  end if
  }
end while
```

Algorithm 1. The pseudo-code of the proposed data forwarding strategy.

with tight social relationships can provide each other with reliable forwarding service of high QoE; hence, a close social relationship signifies high relationship-based credibility. Besides, when two nodes forward data for the same node, the data transmission between them can be achieved through the assistance of this node. Thus, higher similarity of service objective sets means higher relationship-based credibility. Clearly, data can be forwarded with the assistance of socially close nodes. Therefore, relationship-based credibility is defined as the larger of relationship closeness $b_{i,j}(t)$ and service similarity $T_{i,j}^{s,-1}(t)$, where the service similarity indicates that two nodes have provided forwarding service for the same node, that is, the proportion of periods where $Ser_i(T_l) \cap Ser_j(T_l) \neq \phi$ ($Ser_i(T_l)$ is the relay set of node i in the lth movement period to all m movement periods.

In summary, node credibility can be calculated based on process-based and relationship-based credibility. Moreover, weight β is crucial to accurate evaluation of node credibility. Due to the different movement trajectories and activity degrees, the encounter probabilities for node pairs vary greatly, and socially close nodes are more likely to forward data to each other. However, the accurate estimate of the trust status is impossible if it is solely according to the interaction between two remote nodes. Thus, recommendation messages are employed to evaluate relationship-based credibility and to further precisely obtain the trust status of a strange node. Eventually, β can be defined as the ratio of the encounter strength between nodes i and j to the maximum encounter strength of node i.

Trust Status Evaluations

The sparse node distribution of an ICWN will lead to limited encounter times between nodes. Apparently, locally recorded trust information is not suitable for accurate credibility evaluation. Meanwhile, process-based credibility is based on the direct interaction between nodes, which cannot accurately reflect the actual credibility and may result in increased delays or even delivery failures. Recommendation messages from neighbors can effectively mitigate the impact of various errors. Therefore, during the trust status evaluation process, the direct interaction and recommendation messages are comprehensively considered to alleviate the credibility distortion caused by computational errors and non-cooperative node behavior. When node i and j encounter each other, the credibility value of node j is updated according to $T_i \cdot T_{i,j}^{dir}(t) + (1 - T_i) \cdot T_{i,j}^{ind}(t)$ by node i, where $T_{i,j}^{dir}(t)$ is the locally calculated direct credibility value, $T_{i,j}^{ind}(t)$ is the recommended indirect credibility value, and T_i is the weight factor defined by

$$\sum_{k \in \Gamma_i} T_{k,i}(t) \Big/ |\Gamma_i|.$$

The trade-off between direct and indirect credibility is determined by the weight.

QoP-Driven Data Forwarding

Data are forwarded in an ICWN through the cooperation of multiple relays in the "store-carry-forward" manner; thus, reasonably selected relays can achieve efficient data transmission and improved user QoE, while reducing the communication overhead. However, malicious nodes intentionally discard received data, which has a negative impact on the network QoP and user QoE, and wastes precious encounter probabilities and network resources. Thus, the key to designing a data forwarding mechanism for an ICWN lies in the effective utilization of limited network resources. Obviously, data forwarded to trusted nodes are guaranteed to be delivered. Meanwhile, selecting relays with close relationships to the destination node can dramatically improve the delivery ratio and delay performance, while avoiding unnecessary data forwarding and optimizing network resource utilization and QoP.

To achieve reliable data transmission in an ICWN with malicious nodes, the social relationship between nodes is fully exploited to design a QoP-driven data forwarding strategy. With the assistance of recommendation messages from neighbors, and the evaluated process-based and relationship-based credibility, the final credibility of nodes can be obtained, and the relays can be reasonably selected to forward and deliver data. The detailed forwarding process is illustrated in Fig. 2.

When the connection is established between nodes, the encounter strength is calculated, and the neighbor lists are updated accordingly.

The data carrying node i (including the source and relay nodes) judges whether the encountered node j is the destination node. If so, the delivery is accomplished. Otherwise, the process-based and relationship-based credibility $T_{i,j}^{beh}(t)$ and $T_{i,j}^{s}(t)$ are separately calculated to obtain the direct credibility $T_{i,j}^{dir}(t)$ of node j.

To reduce errors in credibility evaluation, node i requests the recommendation message about node $jT_{k,j}^{dir}(t)$ from its neighbor k, and the

final credibility of node j can be updated according to the hybrid credibility update method.

If the final credibility of node j is smaller than 0.5, the data of node i will not be forwarded to node j. Otherwise, if the credibility of node j T_j or the social relationship strength with destination $b_{j,d}(t)$ are larger than those of node i, the data will be forwarded. However, if the above two conditions are not met, the data carrying node will wait until it encounters the proper relay. The pseudo-code of the proposed data forwarding strategy is shown in Algorithm 1.

Numerical Analysis

To verify the validity of the proposed mechanism and network QoP performance, the Opportunistic Network Environment (ONE) [16] simulation platform is employed, in this article and the comparison is done with the classic Prophet and representative Trust-Thresholds [8]. The historical interaction information and multidimensional attributes are exploited to evaluate the node credibility in Trust-Thresholds, and then the threshold mechanism can select the trust information recommending the node and relay nodes to finally accomplish the data forwarding decision. The performance metrics include the data delivery ratio, QoP, transmission cost, and average transmission delay, where QoP is the proportion of data forwarded to general (non-malicious) nodes to the total number of forwarded data, and the transmission cost is the total forwarding times of successful data delivery.

In this section, a map-based community model evaluation method is utilized. A map-based community model restricts the movements of nodes to actual streets within an imported map. In our simulation, we use a map of a 4500 m × 3400 m section of Helsinki, Finland, which contains 96 opportunistic Bluetooth contacts (nodes), and the transmission range is set to 10 m. Transmission speed for all the nodes is set to 250 kb/s. We also assume that the data interval follows exponential distribution within the range of [30, 40] s, and the cache capacity of each node varies from 5 to 10 MB.

QoP

Figure 3 depicts the trend of QoP under different proportions of malicious nodes for the three mechanisms. Clearly, an increasing proportion of malicious nodes will cause increased amounts of discarded data, an increased ratio of attacked data, and reduced network QoP. Of the three mechanisms, Trust-Thresholds can evaluate node credibility according to node behaviors and recommendation messages, which can withstand malicious attacks to some extent. However, the social relationship between nodes is not considered, and the fixed threshold cannot suit the dynamic ICWN, which restrains its availability. The proposed QoP-DF exploits social relationships, evaluates node credibility, and introduces an intrusion detection mechanism to reasonably select relay nodes, avoid random data forwarding, and fully utilize the network resource. Compared to Prophet and Trust-Thresholds, the QoP of QoP-DF is 19.7 and 7.1 percent higher, and its decrease speed is relatively low. When the ratio of malicious nodes reaches 50 percent, the proposed QoP-DF can still provide QoP higher than 70 percent. In conclusion, the negative impact of malicious nodes can be effectively alleviated by the proposed mechanism, and a relatively high QoP can be sustained in a malicious network environment.

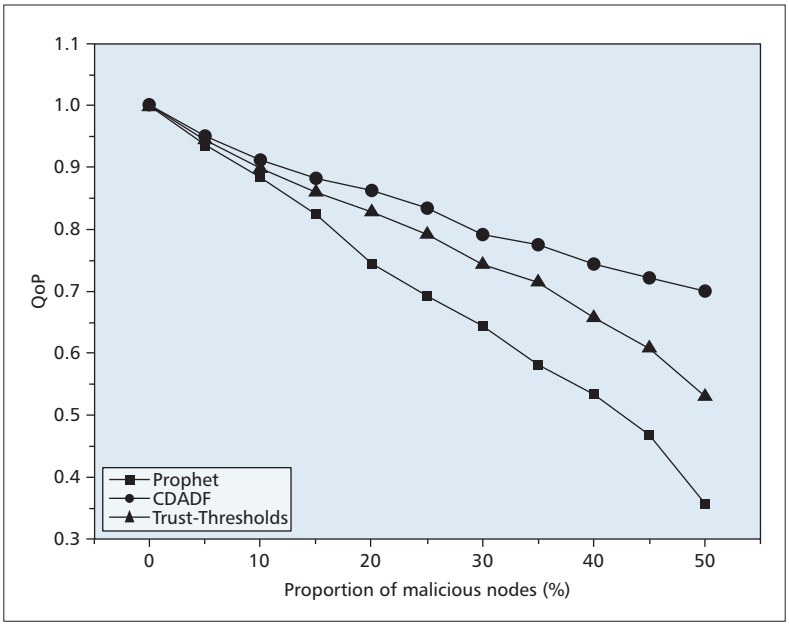

Figure 3. The QoP under different proportions of malicious nodes.

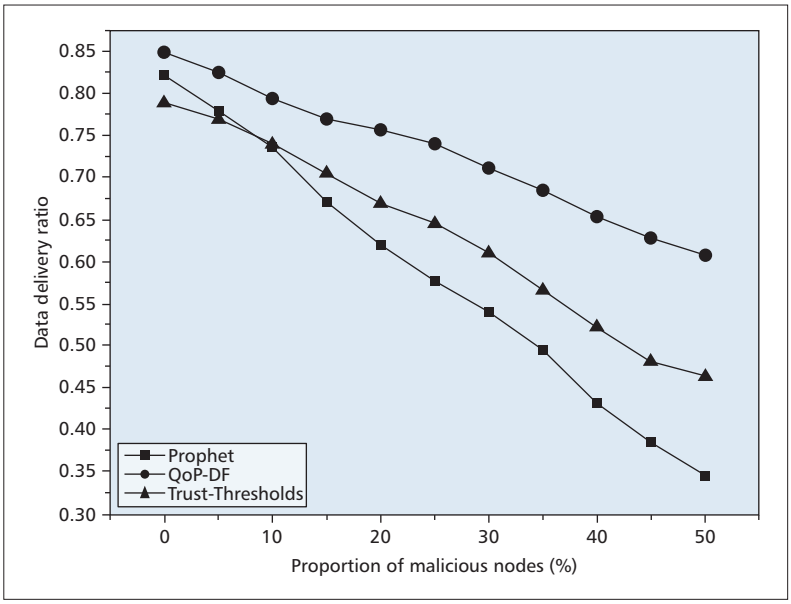

Figure 4. Data delivery ratio under different proportions of malicious nodes.

Data Delivery Ratio

The trend of the data delivery ratio is illustrated in Fig. 4. Along with the increasing proportion of malicious nodes, data are prone to be intercepted and discarded, which results in a reduced delivery ratio. Due to the comprehensive consideration of node behaviors and social relationships, QoP-DF provides 25.6 and 15.2 percent

higher data delivery ratio compared with Prophet and Trust-Thresholds. Besides, QoP-DF can guarantee at least 60 percent delivery ratios even when the proportion of malicious nodes reaches 50 percent.

Transmission Cost

The data transmission efficiency under different proportions of malicious nodes is shown in Fig. 5. Along with increasing malicious node proportion, transmission cost rises due to the intercepted and discarded data copies and increased retransmission times. Besides, the relay node selection processes of QoP-DF and Trust-Thresholds lead to smooth growth of their transmission costs. The proposed QoP-DF can accurately evaluate the node credibility and reasonably select relays, so its transmission cost is 25.0 and 19.3 percent lower compared to Prophet and Trust-Thresholds.

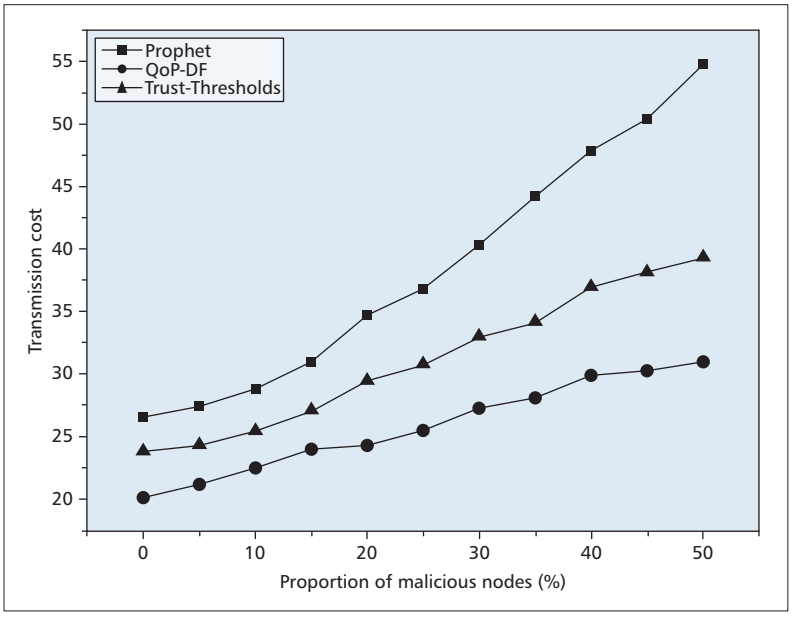

Figure 5. Transmission cost under different proportions of malicious nodes.

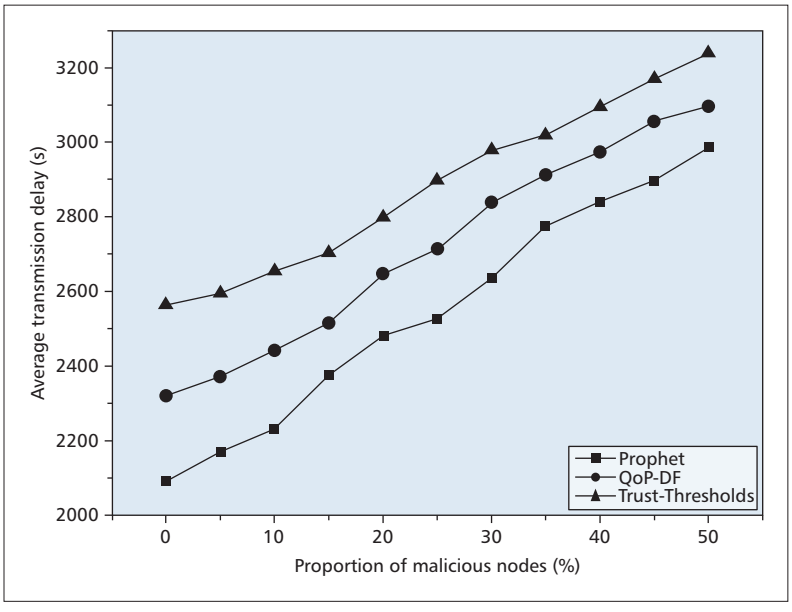

Figure 6. Average transmission delay under different proportions of malicious nodes.

Average Transmission Delay

Along with the increasing malicious node proportion, the average transmission delay rises due to the retransmissions caused by discarded data. Obviously, the proposed QoP-DF can provide 5.6 percent lower average transmission delay than that of Trust-Thresholds. However, when compared to Prophet, the average transmission delay is 7.0 percent higher.

In conclusion, when transmitting packets under scenarios with malicious nodes, data can probably be intercepted and discarded, which causes decreased QoP and a waste of network resources. The proposed QoP-DF evaluates both process-based and relationship-based credibility, and introduces a dynamic intrusion detection mechanism to facilitate malicious node identification, by which reliable relays with high forwarding abilities can be selected. Eventually, even though the transmission delay of QoP-DF is slightly higher than that of Prophet due to the wait time for proper relay nodes and the aggregation time for recommendation messages, QoP-DF can provide high QoP and user QoE with low network load under malicious environments.

Conclusion

In the resource limited ICWN, the existence of malicious nodes greatly degrades the network reliability, resource utilization, network QoP, and user QoE. By analyzing the social relationship between nodes and forwarding behaviors, a QoP-driven data forwarding strategy is proposed in this article. Our major contributions in the article include:

1. The relationship strength is estimated according to the locally recorded encounter history.
2. Process-based and relationship-based credibility are evaluated, and the final node trust status is obtained with the assistance of the dynamical intrusion detection and hybrid credibility update methods.

Based on the results of 1 and 2, the data forwarding decision can be accomplished with improved network performance. Our simulation results show that the QoP and user QoE can be improved dramatically by the proposed QOP-DF, and then the effectiveness of our proposed approach is verified.

Acknowledgment

This work is supported in part by the National Natural Science Foundation of China (61371097), Chongqing Natural Science Foundation (Grant No. CSTC2013JJB40001, CSTC2013JJB40006), Youth Talents Training Project of Chongqing Science & Technology Commission (cstc2014kjrc-qnrc40001).

References

[1] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges." *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 2, 2012, pp. 607–40.

[2] Z. Zhang, "Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges." *IEEE Commun. Surveys & Tutorials*, vol. 8, no. 1, 2006, pp. 24–37.
[3] S.N. Foley *et al*., "Multilevel Security and Quality of Protection," *Proc. First Workshop on Quality of Protection*, Como, Italy, Sept. 2005.
[4] V. S. Mota, F. D. Cunha, and D. F. Macedo, "Protocols, Mobility Models and Tools In Opportunistic Networks: A Survey," *Computer Commun.*, vol. 48, no. 4, 2014, pp. 5–19.
[5] H. J. Zhu *et al*., "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks," *IEEE Trans. Parallel Distrib. Sys*., vol. 25, no. 1, 2014, pp. 22–32.
[6] R. Savola and J. Roning, "Towards Security Evaluation Based on Evidence Collection," *Proc. Third Int'l Conf. Fuzzy Systems and Knowledge Discovery*, Xi'an, China, Sept. 24–28, 2006, pp. 1178–81.
[7] H. J. Zhu *et al*., "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," *IEEE Trans. Vehic. Tech*., vol. 58, no. 8, 2009, pp. 4628–39.
[8] I. Chen *et al*., "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," *IEEE Trans. Parallel Distrib. Sys*., vol. 25, no. 5, 2013, pp. 1200–10.
[9] F. Li, J. Wu, and Srinivasan A, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," *Proc. IEEE INFOCOM '09*, 2009, pp. 2428–36.
[10] N. Li and S. K. Das, "A Trust-Based Framework for Data Forwarding in Opportunistic Networks," *Ad Hoc Networks*, vol. 11, no. 4, 2011, pp. 1497–1509.
[11] X. Wang, L. Liu, and J. Su. "Rlm: A General Model for Trust Representation and Aggregation," *IEEE Trans. Services Computing*, vol. 5, no. 1, 2012, pp. 131–43.
[12] E. Ayday and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary *Detection for Delay-Tolerant Networks," IEEE Trans. Mobile Computing*, vol. 11, no. 9, 2012, pp. 1514–31.
[13] M. K. Denko, T. Sun, and I. Woungang, "Trust Management In Ubiquitous Computing: A Bayesian Approach," *Computer Commun.*, vol. 34, no. 3, 2011, pp. 398–406.
[14] B. Eyuphan and K. Boleslaw, "Exploiting Friendship Relations for Efficient Routing in Mobile Social Networks," *IEEE Trans. Parallel Distrib. Sys*., vol. 23, no. 12, 2012, pp. 2254–65.
[15] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE Rap: Social-Based Forwarding in Delay-Tolerant Networks," *IEEE Trans. Mobile Computing*, vol. 10, no. 11, 2011, pp. 1576–89.
[16] A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," *Proc. ICST*, 2009, pp. 1–10.

Biographies

Dapeng Wu (wudapengphd@gmail.com) received his M.S. degree in communication and information systems in June 2006 from Chongqing University of Posts and Telecommunications, and his Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT) in 2009. He is currently a professor at Chongqing University of Posts and Telecommunications. His research interests include ubiquitous networks, IP QoS architecture, network reliability, and performance evaluation in communication systems.

Hongpei Zhang received his B.S. degree in information and computing science in June 2008 from Henan University of Technology. He is now a Master's degree candidate in information and communication engineering at Chongqing University of Posts and Telecommunications. His research interests include intermittently connected wireless networks, routing protocol, and network security.

Honggang Wang (hwang1@umassd.edu) worked for Bell Labs Lucent Technologies China from 2001 to 2004 as a member of technical staff. He received his Ph.D. in computer engineering from the University of Nebraska-Lincoln in 2009. He is currently an assistant professor at the University of Massachusetts Dartmouth and is an affiliated faculty member of the Advanced Telecommunications Engineering Laboratory at the University of Nebraska-Lincoln. He is also a faculty member of the Biomedical Engineering and Biotechnology Ph.D. program at the University of Massachusetts Dartmouth. His research interests include wireless health, body area networks, cyber security, mobile multimedia and cloud, wireless networks and cyber-physical systems, and big data in mHealth.

Chonggang Wang (cgwang@ieee.org) received a Ph.D. degree from BUPT in 2002. He is currently with InterDigital Communications. His R&D focuses on the Internet of Things, machine-to-machine communications, future Internet, and mobile networks, including technology development and standardization. Before joining InterDigital in 2009, he performed R&D at NEC Laboratories America, AT&T Labs Research, the University of Arkansas-Fayetteville, and Hong Kong University of Science and Technology.

Ruyan Wang received his Ph.D. degree in 2007 from the University of Electronic and Science Technology of China and his M.S. degree from Chongqing University of Posts and Telecommunications (CQUPT), China, in 1997. From December 2002, he is a professor at the Special Research Centre for Optical Internet and Wireless Information Networks at CQUPT. His research interests include network performance analysis and multimedia information processing.

Yi Xie is currently a professor-level senior engineer at the China Academy of Telecommunication Research of MIIT, China. His research interests include ubiquitous networks, network performance analysis, and network reliability.

Even though the transmission delay of QoP-DF is slightly higher than that of Prophet due to the wait time for proper relay nodes and the aggregation time for recommendation messages, QoP-DF can provide high QoP and user QoE with low network load under malicious environments.